

FORM PTO-1449 U.S. DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE INFORMATION DISCLOSURE STATEMENT BY APPLICANT	ATTY DOCKET NO. 20206-0014(PT-TA-410)	PATENT NO. 5,848,159
	APPLICANT COLLINS et al.	
	ISSUE DATE December 8, 1998	GROUP 2766

U. S. PATENT DOCUMENTS

EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME	CLASS	SUBCLASS	FILING DATE IF APPROPRIATE
	AA	5,761,310	06/1998	Naciri	380	30	07/18/1996

FOREIGN PATENT DOCUMENTS

		DOCUMENT NUMBER	DATE	COUNTRY	NAME	CLASS	SUBCLASS	TRANSLATION YES NO
	AB							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

JWS	AC	S.A. VANSTONE et al., "Using Four-Prime RSA in Which Some of the Bits are Specified," December 8, 1994, Electronics Letter, Vol. 30, No. 25. pp. 2118-2119
JWS	AD	C. Couvruer et al., "An Introduction to Fast Generation of Large Prime Numbers," 1982, Philips Journal of Research, Vol. 37, Nos. 5-6, pp. 231-264.
JWS	AE	Y. DESMEDT et al., "Public-Key Systems Based on the Difficulty of Tampering (Is There a Difference Between DES and RSA?)," 1986, Lecture Notes in Computer Science, Advances in Cryptology-CRYPTO '86 Proceedings.
JWS	AF	J. J. QUISQUATER et al., "Fast Decipherment Algorithm for RSA Public-Key Cryptosystem" October 1982, Electronic Letters, Vol. 19, No. 21.
JWS	AG	CETIN KAYA KOC, "High-Speed RSA Implementation (Version 2.0)," November 1994, RSA White Paper, RSA Laboratories.
JWS	AH	RIVEST et al., "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems," February 1978, Communications of the ACM, Vol. 21.
JWS	AI	PKCS #1: RSA Encryption Standard (Version 1.5), November 1993, RSA Laboratories Technical Note.
JWS	AJ	M.O. RABIN, "Digitalized Signatures and Public-Key Functions as Intractable as Factorization," January, 1979, MIT Laboratory for Computer Science.
JWS	AK	R. LIDL et al., "Permutation Polynomials in RSA-Cryptosystems," 1984, Advances in Cryptology—Crypto '83, pp. 293-301.
JWS	AL	D. BONEH et al., "Generating a Product of Three Primes with an Unknown Factorization," Computer Science Department, Stanford University.
JWS	AM	J. J. QUISQUATER et al., "Fast Generation of Large Prime Numbers" June 1982, Library of Congress, Catalog No. 72-179437, IEEE Catalog No. 82CH1767-3 IT, pp. 114-115
JWS	AN	A. J. Menezes et al., "Handbook of Applied Cryptography", 1997, Library of Congress catalog No. 96-27609, pp. 89, 612-613

